James E. Cecchi
CARELLA, BYRNE, CECCHI,
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

[Additional Attorneys on Signature Page]

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FRANKIE J. GONZALEZ, Individually And On Behalf Of All Others Similarly Situated,

Plaintiff,

v.

T-MOBILE US, INC.,

Defendant.

Case No. _____

COMPLAINT AND
DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiff Frankie J. Gonzalez ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against T-Mobile US, Inc. ("T-Mobile" or the "Defendant"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based on, among other things, the investigation of counsel, and a review of public documents.

I. NATURE OF THE ACTION

1. With over 100 million customers, T-Mobile is one of the largest consumer brands in the United States. It collects vast troves of personal information from its customers and prospective customers and profits from that data through its own marketing efforts and by selling sensitive consumer information to third parties. T-Mobile understood it had an enormous responsibility to protect the data it collected and assured consumers through its Privacy Policy that T-Mobile uses "administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control." Its Privacy Center likewise assured consumers that "[w]ith T-Mobile, you don't have to worry," "[w]e've got your back," and "you can trust us to do the right thing with your data." But, as T-Mobile admitted, it completely failed to meet these obligations and protect sensitive consumer data. Instead, T-Mobile suffered a ***second*** colossal data breach impacting the sensitive personal information of 37 million customers—announced just one day after settling one of the largest and most consequential data breaches in U.S. history.[1]

2. On January 19, 2023, T-Mobile revealed the company's second major breach in less than two years, admitting that a hacker was able to obtain customer data, including names, birth dates, and phone numbers, from 37 million accounts (the "Data Breach").[2] T-Mobile said in

[1] Jess Weatherbed, *T-Mobile announces another data breach, impacting 37 million accounts*, THE VERGE (Jan. 20, 2023) available at: https://www.theverge.com/2023/1/20/23563825/tmobile-data-breach-api-customer-accounts-hacker-security (last accessed: Jan. 23, 2023).

[2] *See* Exhibit A, Form 8-K filed by T-Mobile US, Inc. with the SEC on January 19, 2023 ("Ex.

a filing with the Securities and Exchange Commission ("SEC") on January 19, 2023 that it currently believes the attacker first retrieved the data around November 25, 2022, through one of its APIs.[3]

3. T-Mobile stated it detected malicious activity on January 5, 2023 and that the attacker had access to the exploited API for over a month.[4] T-Mobile said it traced the source of the malicious activity and fixed the API exploit within a day of the detection. And claimed that the API used by the hacker did not allow access to data that contained any social security numbers, credit card information, government ID numbers, passwords, PINs, or financial information.[5]

4. T-Mobile has disclosed ***eight hacks since 2018***, with previous breaches exposing customer call records in January 2021, credit application data in August 2021, and an "unknown actor" accessing customer info and executing SIM-swapping attacks in December 2021.[6] In April last year, the hacking group Lapsus$ stole T-Mobile's source code after purchasing employees' credentials online.[7] T-Mobile's failure to implement industry-standard security protocols and its repeated failure to detect and secure customer information have caused harm to Plaintiff and the Class.[8]

5. As a result of T-Mobile's actions, Plaintiff and the Class experienced damages from: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) T-Mobile's

---

A").
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Weatherbed, *T-Mobile announces another data breach*, THE VERGE.
[7] *Id.*
[8] *Id.*

retention of profits attributable to Plaintiff's and other customers' PII that T-Mobile failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff are now exposed to; (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach; and (viii) overpayments of T-Mobile's products and/or services which Plaintiff purchased.

II. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 (d)(2). If a class is certified in this action, the amount in controversy will exceed $5,000,000.00, exclusive of interest and costs. There are more than 100 members in the proposed class, and at least one member of the proposed class is a citizen of a state different from T-Mobile.

7. This Court has personal jurisdiction over T-Mobile because it conducts business in the State of New Jersey, purposefully directs or directed its actions toward New Jersey, and/or has the requisite minimum contacts with New Jersey necessary to permit the Court to exercise jurisdiction. This Court also has personal jurisdiction over T-Mobile because T-Mobile's conduct caused harm to thousands of Class members residing in New Jersey.

8. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(2), a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated in this District. T-Mobile's conduct caused harm to thousands of Class members residing in New Jersey.

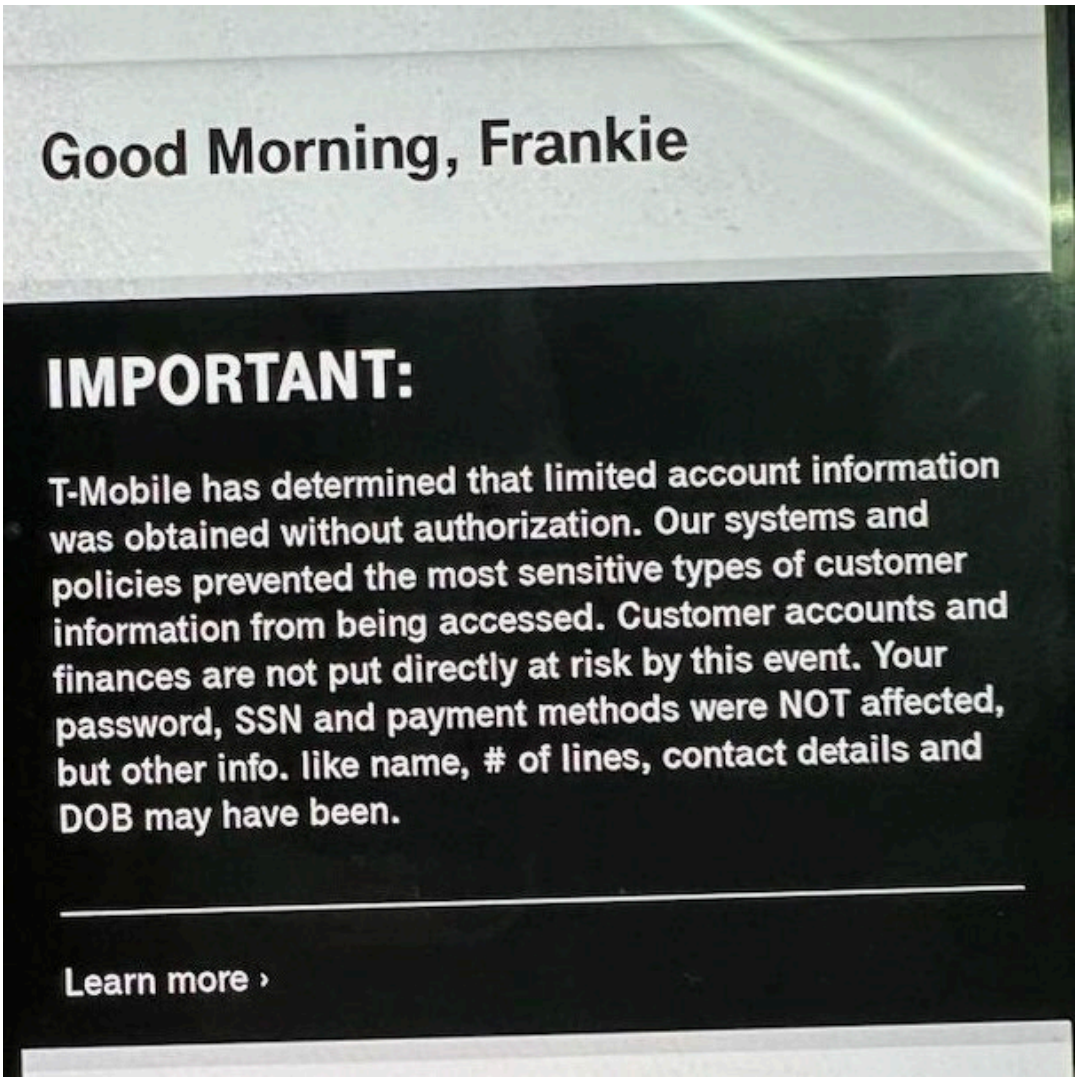
III. PARTIES

A. Named Plaintiff

9. Plaintiff Frankie J. Gonzalez is an individual who had his personally-identifiable information ("PII") exfiltrated and compromised in the Data Breach announced by T-Mobile on

January 19, 2023, and he brings this action on behalf of himself and all those similarly situated both across the United States and within New Jersey. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only T-Mobile (and the hackers) have knowledge of what information was compromised.

10. Plaintiff is a resident of the State of New Jersey and is a current T-Mobile customer with two cellular phone lines and two smartwatch cellular lines. Plaintiff was notified of the Data Breach by T-Mobile through a banner linked to his account that stated the following:



11. Plaintiff is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff places significant value in the security of his PII. Plaintiff entrusted his sensitive PII to T-Mobile with the understanding that T-Mobile would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. If Plaintiff had known of T-Mobile's lax security practices with respect to Plaintiff's PII, he would not have done business with T-Mobile, would not have applied for T-Mobile's services or purchased its products, would not have opened, used, or continued to use T-Mobile's cell phone and other telecommunications-related services at the applicable rates and on the applicable terms, or would have paid less at the point-of-sale of T-Mobile's services.

B. Defendant

12. Defendant T-Mobile US, Inc. is incorporated in the state of Delaware with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006. Defendant is a national telecommunications company that provides mobile communication services, among other products and services, throughout the United States and around the globe.

IV. FACTUAL BACKGROUND

A. T-Mobile is One of the Largest Wireless Cellphone Carriers in the United States

13. T-Mobile provides wireless voice, messaging, and data services in the United States mainland including Alaska, Hawaii, Puerto Rico and the U.S. Virgin Islands under the T-Mobile and Metro by T-Mobile brands. The company operates the second largest wireless network in the U.S. market with over 95 million customers and annual revenues of $32 billion. Its nationwide network reaches 98 percent of Americans, through its EDGE 2G/HSPA 3G/HSPA+ 4G/4G LTE networks, as well as through roaming agreements.

14. The company owns licenses to operate a 1900 MHz GSM PCS digital cellular

network and AWS UMTS digital cellular networks using 600 MHz, 700 MHz, 850 MHz, 1700 MHz and 2100 MHz covering areas of the continental U.S., Alaska, Hawaii, Puerto Rico and the U.S. Virgin Islands. It provides coverage in areas where it does not own radio frequency spectrum licenses via roaming agreements with other operators of compatible networks. In addition to its cellular mobile network, T-Mobile operates a nationwide Wi-Fi Internet-access network under the T-Mobile HotSpots brand.

15. T-Mobile traces its roots to the 1994 establishment of VoiceStream Wireless PCS as a subsidiary of Western Wireless Corporation. Spun off from parent Western Wireless on 3 May 1999, VoiceStream Wireless Corporation was purchased by Deutsche Telekom on 31 May 2001, for $35 billion and renamed T-Mobile US, Inc. in July 2002. This legacy is reflected in some mismatch between US and German T-Mobile service, notably the frequency mismatch making phones inoperative in the other country, and picture messaging issues (non-delivery of pictures in text messages) between those networks. On May 1, 2013, the combined company, now known as T-Mobile US, began trading on the New York Stock Exchange as a public company.

B. T-Mobile Has a History of Data Breaches

16. The Data Breach and resulting harm suffered by Plaintiff and Class Members is directly attributable to T-Mobile's history of security lapses and data mismanagement. Indeed, T-Mobile is no stranger to cybersecurity incidents resulting from its flawed security. Rather, data breaches have been a nearly annual event for the company for many years.

17. In 2017, Karan Saini, a security researcher, found a bug on a T-Mobile website that allowed hackers to access PII like email addresses, account numbers, and IMSI numbers, just by knowing or guessing a customer's phone number.[9] According to Saini, "T-Mobile has 76 million

[9] Lorenzo Franceschi-Bicchierai, *T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number*, Motherboard (Oct. 10, 2017), available at

customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users."[10] Saini explained "[t]hat would effectively be classified as a very critical data breach, making every T-Mobile cell phone owner a victim."[11] T-Mobile had no mechanism in place to prevent this type of critical data breach, according to Saini.[12] According to a hacker, the bug had been exploited by multiple hackers over a multi-week period before it was discovered by Saini.[13] In fact, the hackers who found the bug before Saini went so far as to upload a tutorial on how to exploit it on YouTube.[14]

18. In 2018, hackers gained access to T-Mobile servers and stole the PII of roughly two million T-Mobile customers.[15] The stolen PII included names, email addresses, account numbers, other billing information, and encrypted passwords.[16] T-Mobile misleadingly downplayed the hack, claiming that no passwords were "compromised."[17] In truth, the hackers stole millions of encrypted passwords that were likely decrypted by the hackers due to the weak encoding algorithm employed by T-Mobile, leading one security expert to advise affected customers to assume their passwords were cracked and change them as a result.[18]

---

https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] Lorenzo Franceschi-Bicchierai, *Hackers Stole Personal Data of 2 Million T-Mobile Customers*, Motherboard (Aug, 23, 2018), available at https://www.vice.com/en/article/a3qpk5/t- mobile-hack-data-breach-api-customer-data.

[16] *Id.*

[17] *Id.*

[18] *Id.*

19. In November 2019, hackers accessed the PII of roughly 1 million T-Mobile prepaid customers.[19] The PII in that breach included names, phone numbers, addresses, account information, and rate, plan and calling features (i.e., paying for international calls).[20]

20. In March 2020, T-Mobile disclosed it was subject to a data breach that exposed customer and employee PII, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers and billing account information.[21] Later in 2020, T-Mobile suffered yet another data breach in which hackers accessed customer proprietary network information (CPNI) and undisclosed call-related information for hundreds of thousands of customers.[22]

21. Therefore, it is no surprise that in August 2021, The Washington Post reported that "[u]nfortunately, dealing with data breaches is nothing new for the company – or its customers. For those keeping count, this is the fifth such incident the wireless carrier has suffered in the past three years, but according to Allie Mellen, a security and risk analyst at Forrester Research, this is 'the worst breach they've had so far.'"[23]

22. There were more security incidents even after this Breach. In December 2021, T-Mobile disclosed that several customers had experienced SIM-swap attacks, stating: "We informed

---

[19] Devin Coldeway, *More Than 1 Million T-Mobile Customers Exposed by Breach*, TechCrunch (Nov. 22, 2019), available at https://techcrunch.com/2019/11/22/more-than-1- million-t-mobile-customers-exposed-by-breach/.

[20] *Id.*

[21] *T-Mobile Breach Leads to The Exposure of Employee Email Accounts and User Data*, Identity Theft Resource Center (Mar. 5, 2020), available at https://www.idtheftcenter.org/t- mobile-breach-leads-to-the-exposure-of-employee-email-accounts-and-user-data/.

[22] Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call- Related Information of 200,000 Subscribers*, CPO Magazine (Jan. 11, 2021), available at https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/.

[23] Chris Velazco, *Here's What to Do If You Think You're Affected by T-Mobile's Big Data Breach*, Wash. Post (Aug. 19, 2021), available at https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/.

a very small number of customers that the SIM card assigned to a mobile number on their account may have been illegally reassigned or limited account information was viewed."[24]

23. In April 2022 it was announced that members of the LAPSUS$ cybercrime group breached T-Mobile multiple times in March, stealing source code for a range of company projects and accessing employee accounts with access to Atlas, a powerful internal T-Mobile tool for managing customer accounts.[25]

24. Finally, and most recently, on January 19, 2023, T-Mobile announced the Data Breach impacting 37 million customer accounts.

25. Given the numerous data breaches pre-dating the Breach at issue in this case, T-Mobile was clearly aware of its data security failures, and the fact that subsequent breaches have occurred reinforces that Plaintiff's PII, which remains in T-Mobile's possession, is not safe.

C. The Data Breach

26. On January 19, 2023, T-Mobile announced the Data Breach in a filing with the Securities and Exchange Commission ("SEC"). *See* Ex. A.

27. The announcement stated that on January 5, 2023, T-Mobile identified that a "bad actor" obtained data through a single Application Programming Interface ("API") without authorization. *Id.*

28. T-Mobile commenced an investigation with third-party cybersecurity experts and within a day of learning of the malicious activity, and were able to trace the source of the malicious activity and purportedly stopped it. *Id.*

[24] Lori Grunin, *T-Mobile Suffers Another, Smaller Data Breach*, CNET (Dec. 29, 2021), available at https://www.cnet.com/tech/mobile/t-mobile-reportedly-suffers-another-smaller-data- breach/.
[25] Brian Krebs, *Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code*, KrebsOnSecurity (April 22, 2022), available at https://krebsonsecurity.com/2022/04/leaked- chats-show-lapsus-stole-t-mobile-source-code/.

29. T-Mobile stated that their investigation is still ongoing. *Id.*

30. T-Mobile stated that, based on their investigation to date, the impacted API provided customer account data, including name, billing address, email, phone number, date of birth, T-Mobile account number and information such as the number of lines on the account and plan features. *Id.*

31. The preliminary result from T-Mobile's investigation indicates that the bad actor(s) obtained data from this API for approximately 37 million current postpaid and prepaid customer accounts. *Id.*

32. T-Mobile stated it believes the bad actor first retrieved data through the impacted API starting on or around November 25, 2022. *Id.*

33. T-Mobile stated it may incur significant expenses in connection with this incident.

D. Consequences of the Data Breach for Consumers

34. Plaintiff and the Class have suffered actual harm and will continue to be harmed as a result of T-Mobile's conduct. T-Mobile failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. This breach may allow hackers to access the PII, including first and last names, postal addresses, email addresses, and telephone numbers, for Plaintiff and the Class. This PII has since been publicly leaked online, which has allowed for digital and potential physical attacks against Plaintiff and the Class. Now that the PII has been leaked, it is available for other parties to sell or trade and will continue to be at risk for the indefinite future.

35. T-Mobile's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach – names, addresses, zip codes, phone numbers, email addresses and, dates of birth – hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into

the indefinite future. As a result, Plaintiff has suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

36. Plaintiff's stolen PII may now be circulating on the dark web and it is highly valuable. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create synthetic identities.

37. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and identifies the victims as T-Mobile's current, former, or prospective customers materially increases the risk to Plaintiff and the Class.

38. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[26] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data

[26] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07- 737/html/GAOREPORTS-GAO-07-737.htm (last visited Jan. 23, 2023).

Breach is not used to harm them. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach. In other words, Plaintiff have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

39. Plaintiff and Class Members have also realized harm in the lost or reduced value of their PII. T-Mobile admits the PII compromised in the Breach is valuable. As discussed above, T-Mobile collects, retains, and uses Plaintiff's PII to increase profits through predictive and other targeted marketing campaigns. Plaintiff's PII is not only valuable to T-Mobile, but Plaintiff also place value on their PII based on their understanding that their PII is a financial asset to companies that collect it.[27]

40. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiff's PII that was permitted without authorization by T-Mobile. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

41. Moreover, Plaintiff and Class Members value the privacy of this information and expect T-Mobile to allocate enough resources to ensure it is adequately protected. Customers would not have done business with T-Mobile, provided their PII, or paid the same prices for T-Mobile's goods and services had they known T-Mobile did not implement reasonable security measures to protect their PII.[28] Customers reasonably expect that the payments they make to the

[27] *See, e.g.*, *Ponemon Institute, LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities."), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

[28] FireEye, Beyond the Bottom Line: The Real Cost of Data Breaches (May 11, 2016),

carrier, either prepaid or each month, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiff and Class Members did not receive the benefit of their bargain with T-Mobile because they paid a value for services they expected but did not receive.

42. Given T-Mobile's failure to protect Plaintiff's and the Class Members' PII despite multiple data breaches in the past as well as subsequent data breaches, Plaintiff have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII remains in T-Mobile's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

43. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of access to Plaintiff's and Class Members' PII permitted by T-Mobile; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; (vi) T-Mobile's retention of profits attributable to Plaintiff's and Class Members' PII that T-Mobile failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow

---

https://www.fireeye.com/current-threats/cost-of-a-data-breach/wp-real-cost-data-breaches.html (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to T-Mobile for goods and services purchased, as Plaintiff reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and (x) nominal damages.

V. CLASS ACTION ALLEGATIONS

44. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class and a New Jersey Sub-Class, defined as follows:

Nationwide Class

> All persons in the United States whose PII was maintained on the T-Mobile systems that were compromised as a result of the breach announced by T-Mobile on or around January 19, 2023.

New Jersey Sub-Class

> New Jersey Sub-Class: All persons in the State of New Jersey whose PII was maintained on T-Mobile systems that were compromised as a result of the breach announced by T-Mobile on or around January 19, 2023.

45. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

46. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant owed Plaintiff and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII, and whether it breached that duty;

b. Whether Defendant continues to breach duties to Plaintiff and other Class

Members;

c. Whether Defendant's data security systems before the data breach met industry standards;

d. Whether Defendant failed to adequately respond to the data breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay;

e. Whether Plaintiff and other Class Members' PII was compromised in the data breach; and

f. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

47. Plaintiff's claims are typical of the Classes' claims. Plaintiff suffered the same injury as Class Members—i.e., Plaintiff's PII was compromised in the data breach.

48. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel has interests that conflict with those of the proposed Classes.

49. Defendant has engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and other Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

50. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the

prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims.

51. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

VI. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

52. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

53. T-Mobile collected sensitive PII from Plaintiff and Class Members when using T-Mobile products and services.

54. T-Mobile owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing T-

Mobile's security systems to ensure that Plaintiff's and Class Members' PII in T-Mobile's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

55. T-Mobile's duty to use reasonable care arose from several sources, including but not limited to those described herein.

56. T-Mobile had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by T-Mobile's failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, T-Mobile knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

57. T-Mobile's duty to use reasonable security measures also arose as a result of the special relationship that existed between T-Mobile, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted T-Mobile with their PII as part of signing-up for the products and services T-Mobile offers as a major technology and communications company. T-Mobile alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

58. T-Mobile's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as T-Mobile. Various FTC publications and data security breach orders further form the basis of T-Mobile's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

59. T-Mobile's duty also arose from T-Mobile's unique position as one of the largest communications companies in the United States. As a technology company, T-Mobile holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiff and Class Members.

60. T-Mobile admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

61. T-Mobile knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

62. T-Mobile also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require T-Mobile to reasonably safeguard sensitive PII, as detailed herein.

63. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate

or ameliorate the damages caused by T-Mobile's misconduct.

64. T-Mobile breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. T-Mobile breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII in T-Mobile's possession had been or was reasonably believed to have been, stolen or compromised.

65. But for T-Mobile's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised and sold on the dark web.

66. T-Mobile's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII.

67. Plaintiff and Class Members were foreseeable victims of T-Mobile's inadequate data security practices, and it was also foreseeable that T-Mobile's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

68. As a direct and proximate result of T-Mobile's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

69. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

70. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as T-Mobile of failing to use reasonable measures to protect PII.

71. The FTC publications and orders also form the basis of T-Mobile's duty.

72. T-Mobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. T-Mobile's conduct was

particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as T-Mobile, including, specifically the damages that would result to Plaintiff and Class Members.

73. In addition, under state data security statutes, T-Mobile had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII.

74. T-Mobile's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

75. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

76. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

77. T-Mobile breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

78. Plaintiff and Class Members were foreseeable victims of T-Mobile's violations of the FTC Act and state data security statutes. T-Mobile knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

79. But for T-Mobile's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

80. As a direct and proximate result of T-Mobile's negligence *per se*, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 3

BREACH OF CONFIDENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

81. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

82. Plaintiff and Class Members maintained a confidential relationship with T-Mobile whereby T-Mobile undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiff and Class Members to T-Mobile to unauthorized third parties. Such PII was confidential

and novel, highly personal and sensitive, and not generally known.

83. T-Mobile knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

84. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because T-Mobile failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

85. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

86. But for T-Mobile's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. T-Mobile's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

87. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of T-Mobile's unauthorized disclosure of Plaintiff's and Class Members' PII. T-Mobile knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII had serious security vulnerabilities because T-Mobile failed to observe even basic information security practices or correct known security vulnerabilities.

88. As a direct and proximate result of T-Mobile's breach of confidence, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

89. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

90. Plaintiff shared PII with T-Mobile that Plaintiff wanted to remain private and non-public.

91. Plaintiff reasonably expected that the PII they shared with T-Mobile would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

92. T-Mobile intentionally intruded into Plaintiff's and Class Members' seclusion by

disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

93. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, T-Mobile unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

94. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

95. T-Mobile's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

96. As a direct and proximate result of T-Mobile's invasions of privacy, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring,

identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 5

BREACH OF EXPRESS CONTRACT

On Behalf of Plaintiff and the Nationwide Class of Current Customers, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass of Current Customers

97. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein. For the purposes of this claim, Plaintiff and Class Members shall mean natural persons who were current customers of T-Mobile as of January 19, 2023.

98. Plaintiff and Class Members on the one side and T-Mobile on the other formed a contract when Plaintiff and Class Members obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile subject to its Privacy Policy.

99. Plaintiff and Class Members fully performed their obligations under the contracts with T-Mobile.

100. T-Mobile breached its agreement with Plaintiff and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

101. As a direct and proximate result of T-Mobile's breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 6

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

102. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

103. Plaintiff and Class Members entered into an implied contract with T-Mobile when they obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile.

104. As part of these transactions, T-Mobile agreed to safeguard and protect the PII of

Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

105. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that T-Mobile's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class Members believed that T-Mobile would use part of the monies paid to T-Mobile under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

106. Plaintiff and Class Members would not have provided and entrusted their PII to T-Mobile or would have paid less for T-Mobile products or services in the absence of the implied contract or implied terms between them and T-Mobile. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

107. Plaintiff and Class Members fully performed their obligations under the implied contracts with T-Mobile.

108. T-Mobile breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

109. As a direct and proximate result of T-Mobile's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the

compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 7

UNJUST ENRICHMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

110. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

111. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by T-Mobile and that was ultimately stolen in the T-Mobile Data Breach.

112. T-Mobile was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. T-Mobile understood that it was in fact so benefitted.

113. T-Mobile also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon T-Mobile maintaining the privacy and confidentiality of that PII.

114. But for T-Mobile's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with T-Mobile.

115. Because of its use of Plaintiff's and Class Members' PII, T-Mobile sold more services and products than it otherwise would have. T-Mobile was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

116. T-Mobile also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

117. T-Mobile also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' PII.

118. It is inequitable for T-Mobile to retain these benefits.

119. As a result of T-Mobile's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), T-Mobile has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

120. T-Mobile's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

121. It is inequitable, unfair, and unjust for T-Mobile to retain these wrongfully obtained benefits. T-Mobile's retention of wrongfully obtained monies would violate fundamental

principles of justice, equity, and good conscience.

122. The benefit conferred upon, received, and enjoyed by T-Mobile was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for T-Mobile to retain the benefit.

123. T-Mobile's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and Class Members other damages as described herein.

124. Plaintiff has no adequate remedy at law.

125. T-Mobile is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on T-Mobile as a result of its wrongful conduct, including specifically: the value to T-Mobile of the PII that was stolen in the Data Breach; the profits T-Mobile received and is receiving from the use of that information; the amounts that T-Mobile overcharged Plaintiff and Class Members for use of T-Mobile's products and services; and the amounts that T-Mobile should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII.

COUNT 8

DECLARATORY JUDGMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

126. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

127. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

128. An actual controversy has arisen in the wake of the T-Mobile Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff continues to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by T-Mobile.

129. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. T-Mobile continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

130. The Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

131. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lacks an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified

and he will be forced to bring multiple lawsuits to rectify the same conduct.

132. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to T-Mobile if an injunction is issued. Among other things, if another massive data breach occurs at T-Mobile, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures.

133. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

VII. CLAIMS ON BEHALF OF THE STATE SUBCLASS

COUNT 9

NEW JERSEY CONSUMER FRAUD ACT N.J.S.A. § 56:8-1, *ET SEQ.*

Plaintiff, on behalf of the New Jersey Subclass

134. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 - 51 as if fully set forth herein.

135. Plaintiff and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

136. Defendant is a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

137. Defendant's conduct as alleged related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

138. Defendant advertised, offered, or sold goods or services in New Jersey and engaged

in trade or commerce directly or indirectly affecting the citizens of New Jersey.

139. Defendant solicited Plaintiff and Class Members to do business and uniformly and knowingly misrepresented that by joining, their PII was safe, confidential, and protected from intrusion, hacking, or theft.

140. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures.

141. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

142. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' PII in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

143. Defendant failed to provide notice to Plaintiff and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

144. Defendant's acts and omissions, as set forth evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

145. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members are required to expend sums to protect and recover their PII, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII, and thereby suffered

ascertainable economic loss.

146. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action under Federal Rule of Civil Procedure 23, and appointment of Plaintiff as a Class Representative and his counsel of record as Class Counsel;

B. That acts alleged above be adjudged and decreed to constitute negligence and violations of the consumer protection laws of New Jersey;

C. A judgment against Defendant for the damages sustained by Plaintiff and the Classes above, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

2. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

3. Ordering that Defendant audit, test, and train its security personnel regarding any

new or modified procedures;

4. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

5. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendant conduct regular database scanning and securing checks; and

7. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiff and Class Members prejudgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after service of this Complaint;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

IX. JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, requests a jury trial, under Federal Rule of Civil Procedure 38, on all claims so triable.

DATED: January 23, 2023

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
Kevin G. Cooper
Jordan M. Steele*
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Tel.: (973) 994-1700
jcecchi@carellabyrne.com
kcooper@carellabyrne.com
jsteele@carellabyrne.com

Zachary S. Bower*
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
2222 Ponce DeLeon Blvd.
Miami, Florida 33134
Tel.: 973-422-5593
zbower@carellabyrne.com

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road 6th Floor
Ridgefield Park, NJ 07660
Tel.: (973) 639-9100
cseeger@seegerweiss.com
cayers@seegerweiss.com

Linda P. Nussbaum
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
Tel: (917) 438-9189
lnussbaum@nussbaumpc.com

Attorneys for Plaintiff and the Proposed Class

** To be admitted pro hac vice*